Sealed

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CIVIL ACTION NO.

MICROSOFT CORPORATION, H2-PHARMA, LLC, and GATEHOUSE DOCK CONDOMINIUM ASSOCIATION, INC.,

Plaintiffs

v.

DOES 1-7,

Defendants

FILED UNDER SEAL

PLAINTIFFS' EMERGENCY MOTION FOR *EX PARTE* TEMPORARY RESTRAINING ORDER AND RELATED RELIEF

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CIVIL ACTION NO.

MICROSOFT CORPORATION, H2-PHARMA, LLC, and GATEHOUSE DOCK CONDOMINIUM ASSOCIATION, INC.,

Plaintiffs

v.

DOES 1-7,

Defendants

PLAINTIFFS' EMERGENCY MOTION FOR *EX PARTE* TEMPORARY RESTRAINING ORDER AND RELATED RELIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

REQUEST FOR EMERGENCY HEARING

Pursuant to Local Rules 7.1(d) and 7.1(b)(2), Plaintiffs respectfully request oral argument on an emergency basis. Plaintiffs are seeking an emergency hearing and respectfully request a ruling on or before July 8, 2026 due to the nature of the relief requested. As explained more fully below, Plaintiffs seek seizure of Internet domains that are currently being used by Defendants to carry out ongoing violations of law. It will likely take one to two business days for the third-party domain registries at issue to effect any seizure order, and time is of the essence given imminent actions that are expected to occur outside the United States next week. Absent emergency relief, Defendants may learn of these and other proceedings before the Court can grant effective relief and would be in a position to thwart important efforts here and abroad.

Oral argument is desired to address any questions the Court may have regarding Plaintiffs technical evidence or witness submissions. Answers to any such questions may assist the Court in understanding the complex and sophisticated nature of Defendants ongoing cybercriminal scheme and the exigencies underlying Plaintiffs' motion. Plaintiffs submit that a hearing of 20 minutes or less will likely suffice to give the Court clarity on the nature of Defendants scheme and the propriety of Plaintiffs' requested relief.

INTRODUCTION

Plaintiffs Microsoft Corporation ("Microsoft"), H2-Pharma LLC ("H2"), and Gatehouse Dock Condominium Association ("GDCA") respectfully move for emergency *ex parte* relief pursuant to Federal Rule of Civil Procedure 65; the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the Electronic Communications Privacy Act (18 U.S.C. §§ 2701 *et seq*); the Lanham Act (15 U.S.C. §§ 1125); the Copyright Act (17 U.SC. §§ 101), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962(c)); the common law, and the All Writs Act (28 U.S.C. § 1651). Plaintiffs' requested relief is necessary for the investigation, abatement, and

remediation of Defendants' unlawful use of Microsoft's software, trademarks, and victim computers to steal information from Microsoft customers for fraudulent purposes. Because prior notice to Defendants of this application motion would provide Defendants with an opportunity to destroy, move, conceal, or otherwise make inaccessible certain instrumentalities and evidence related to their unlawful activities, Microsoft seeks relief *ex parte* and is filing concurrently herewith a motion to seal this action.[1] *See, e.g., Microsoft Corp. v. Does 1-10*, Case No. 1:25cv2695 (N.D. Ga. May 15, 2025) (applying Eleventh Circuit law and granting *ex parte* relief in similar case that remained sealed until execution of the court's orders).

Defendants are a group of natural persons engaged in a malicious scheme to use pirated versions of Microsoft's Windows Server software to carry out at scale a wide range of malicious activities, including financial fraud. Plaintiffs H2 and GDCA, both Florida corporations, are two of Defendants' many financial fraud victims and have joined Microsoft in this action to put a stop to Defendants ongoing misconduct in this judicial district and beyond. Plaintiffs respectfully request an order:

1. Directing Defendants, their service providers, and/or those acting in concert with them to preserve evidence related to, and to cease from using or permitting to be used the domans "redvds.com" and "redvds.pro";

2. Enjoining Defendants from further violations of the CFAA, ECPA, Lanham Act, Copyright Act, RICO Act, and common law; and

3. Directing Defendants to show cause why they should not be preliminarily enjoined from the violations of law described in this Application and Plaintiffs' Complaint.

If Microsoft's requests for relief are granted, Microsoft will work with its private and public partners to disable Defendants' core infrastructure in a carefully timed and coordinated manner

[1] In addition to threatening the efficacy of these civil proceedings, prior notice to Defendants could also adversely impact pending law enforcement investigations in multiple jurisdictions.

that should put an immediate stop to Defendants' misuse of computers running pirated Microsoft software to carry out fraud on unsuspecting Microsoft customers and other members of the public.

Concurrently with this Application, Plaintiffs are filing *ex parte* motions for expedited discovery and alternative service to ensure that as soon as the requested relief is effected, Microsoft can act promptly and diligently to provide formal notice to Defendants by serving them with all papers in this action via all available means of contacting them. Microsoft will also act promptly to unseal this action and file public redacted versions of the papers in this case once any relief granted by the Court has been effected.

STATEMENT OF FACTS

Overview

Microsoft. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington. Microsoft is a leading provider of technology products and services, including computer software, Internet services, websites, and email services. Declaration of Sean Ensz ("Ensz Decl.") ¶ 2. Microsoft is the owner of U.S. Copyright Registration No. TX0009008683 for the software offered commercially as Windows Server and U.S. Trademark Registrations 1689468 and 7706415 for the marks MICROSOFT® and WINDOWS®, respectively. Declaration of Donal Keating ("Keating Decl.") ¶20. Defendants have used pirated versions of Windows Server and counterfeit Microsoft trademarks to carry out sophisticated financial fraud against unsuspecting victims like H2, GDCA, and many others.

H2. H2 is a corporation duly organized and existing under the laws of the State of Florida with its principal place of business in Montgomery, Alabama. Declaration of Josh Blackwell ("Blackwell Decl.") ¶ 4. H2 is a privately held, fast-growing pharmaceutical company focusing

on the sales, marketing and distribution of branded and generic Rx and non-Rx products. *Id.* ¶ 3. H2's products include chemotherapeutic drugs, seizure medication, asthma medication, children's allergy medication, ulcer medication, antiviral medication, and medicines for treating schizophrenia, bipolar disorder, and depression, among other products. *Id.* ¶ 4. H2's expertise includes navigating the various sales channels across the U.S., and providing safe, reliable, and cost-efficient medications to customers. H2 engages in strategic partnerships with other pharmaceutical companies through in-licensing of legacy or pre-commercial products, co-funding of joint development projects, and other partnerships designed to help bring medicine to people who need it. *Id.* ¶ 3. H2 suffered a multi-million-dollar loss due to financial fraud carried out by Defendants using the software and infrastructure at issue in this Application. Blackwell Decl. ¶ 5; Ensz Decl. ¶ 14.

The tradecraft employed by Defendants to defraud H2 was sophisticated. In early 2025, H2 began discussions with a European supplier about ways for H2 to reduce its transactional costs. Blackwell Decl. ¶ 10. These discussions involved email communications about switching H2's payment mechanism from wire transfers to ACH payments. Unbeknownst to H2, its email system had been compromised in the manner described further below. Defendants monitored H2's communications with its supplier and waited for an opportunity to defraud H2. *Id.* ¶14. After observing H2's email discussions with its supplier, at least DOE 3 used the compromised email account to mislead H2 about H2's ACH inquiry and to misdirect H2's payments. In April 2025, DOE 3 sent to H2 emails providing documentation and instructions to facilitate H2's payment of money to an account that H2 believed belonged to its supplier. In fact, the account was under the control of at least DOE 3. *Id.* ¶¶ 13-16. DOE 3 fraudulently caused H2 to send multiple significant payments of money to the subject account. As a result, H2 sustained a

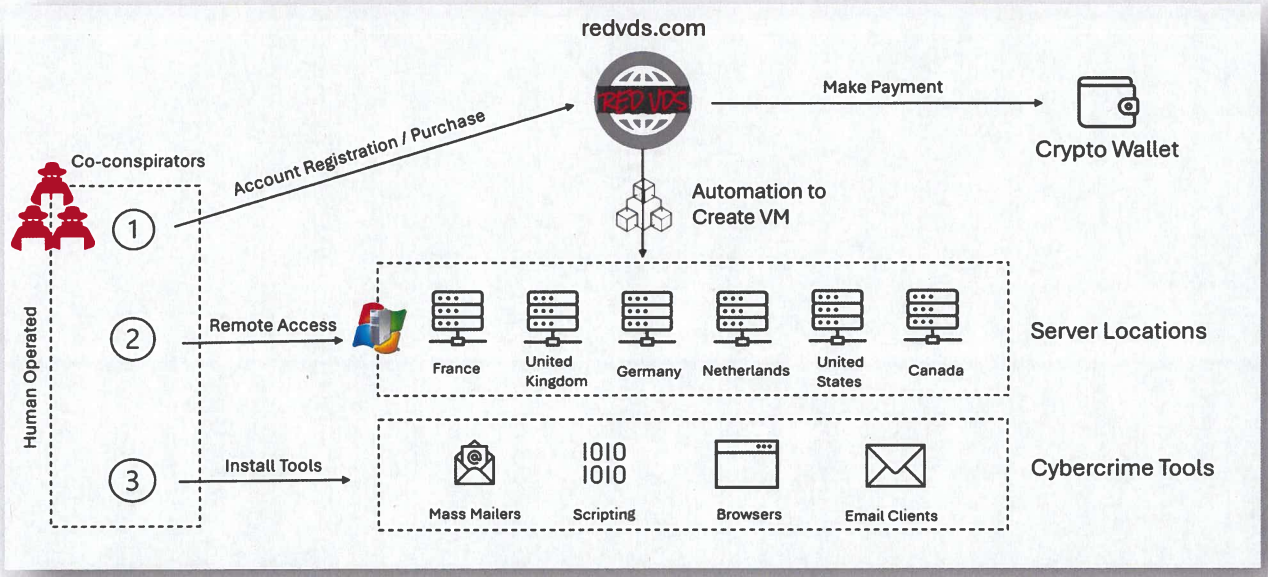
substantial seven-figure loss. H2 only learned that it had been defrauded in May 2025 when its supplier inquired about the status of the payments H2 attempted to send to the supplier. H2 promptly reported DOE 3's crime to law enforcement. *Id.*

GDCA. GDCA is a not-for-profit corporation organized under the laws of the State of Florida with its principal place of business in Key Largo, Florida. Declaration of Geoffrey Noyes ("Noyes Decl.") ¶ 2. GDCA serves as a homeowner's association and is responsible for the management and use of homeowners' association monies to maintain and improve the properties it manages. *Id.* ¶ 3. GDCA suffered several hundred thousand dollars in loss due to financial fraud carried out by Defendants using the software and infrastructure at issue in this Application. Noyes Decl. ¶ 4; Ensz Decl. ¶ 13.

As with the fraud committed on H2, the tradecraft used to defraud GDCA was sophisticated and difficult to detect. In March 2025, Gatehouse and one of its contractors were each in the process of setting up new bank accounts. Around this same time, Gatehouse engaged in email communications and video conferences with its contractor's representative *inter alia* about the timing and routing of payments for services and materials the contractor was providing to Gatehouse. Noyes Decl. ¶¶ 8-10. Gatehouse's contractor stated that it would provide Gatehouse with new bank account information in the coming weeks. Unbeknownst to Gatehouse, the email account of the contractor representative Gatehouse was communicating with had been compromised, and Defendants monitored Gatehouse's communications with its contractor and waited for an opportunity to defraud Gatehouse. *Id.* ¶ 9. After observing Gatehouse's email discussions with its contractor, at least DOE 2 used the compromised contractor email account and a homoglyph of that email account to mislead Gatehouse and to misdirect Gatehouse's payments. *Id.* ¶ 11, Noyes Exhibits 2-4.

In April 2025, DOE 2 sent to Gatehouse an email providing documentation and instructions to facilitate Gatehouse's payment of money to an account that Gatehouse believed belonged to its contractor. Noyes Decl. ¶¶ 13-18. In fact, the account was under the control of at least DOE 2. This email was sent about one week after Gatehouse's contractor told Gatehouse to expect to receive contractor's updated bank account information in about a week. All the while, DOE 2 was monitoring GDCA's private email communications with its supplier. DOE 2 waited for the right moment and then fraudulently caused Gatehouse to send a significant payment of money to the subject account. As a result, Gatehouse sustained a substantial six-figure loss. *Id.* ¶¶20-21.

Defendants. Defendants are the operators, promoters, and users of a marketplace for illegal software and services ("RedVDS Enterprise"). Ensz Decl. ¶¶ 9-23. At the center of Defendants scheme is a website located at the URL redvds[.] com and related subdomains; there is also a backup domain of "redvds.pro" (collectively, the "RedVDS Domains"). The RedVDS Domains facilitate advertising, sales, distribution, hosting, and remote operation of virtual computers running unauthorized copies of Microsoft's Windows Server software. Together, these virtual computers and unauthorized Windows Servers copies comprise a malicious network ("RedVDS Network") that is used by cybercriminals to operate malicious phishing, business email compromise, and financial fraud schemes at scale. *Id.* at 8. Figure 5 from the Declaration of Sean Ensz depicts the technical architecture of the RedVDS Enterprise and RedVDS Network:



Defendants' Piracy of Microsoft's Windows Server Software

The software at issue in this case is known as Windows Server 2022. Windows Server is Microsoft's enterprise server platform that enables organizations to run and secure applications, services, and workloads across on-premises, hybrid, and cloud environments. From a user interface perspective, Windows Server is similar to the common version of Windows that most users are familiar with, but Windows Server has additional features designed to help manage data and applications across multiple computers. Keating Decl. ¶ 4.

Like many Microsoft products, Windows Server is a software product that is licensed, not sold to end users. In order to lawfully use Windows Server, users must agree to a license agreement that requires, among other things, an agreement not to use Microsoft's software for harmful purposes. One element of Microsoft's licensing program is a crypotgraphically generated key, sometimes referred to as a product key, license key, or license certificate ("Windows Server Key"). Windows Server Keys are unique alphanumeric codes used to validate the license status of a copy of Windows Server. Keating Decl. ¶ 4.

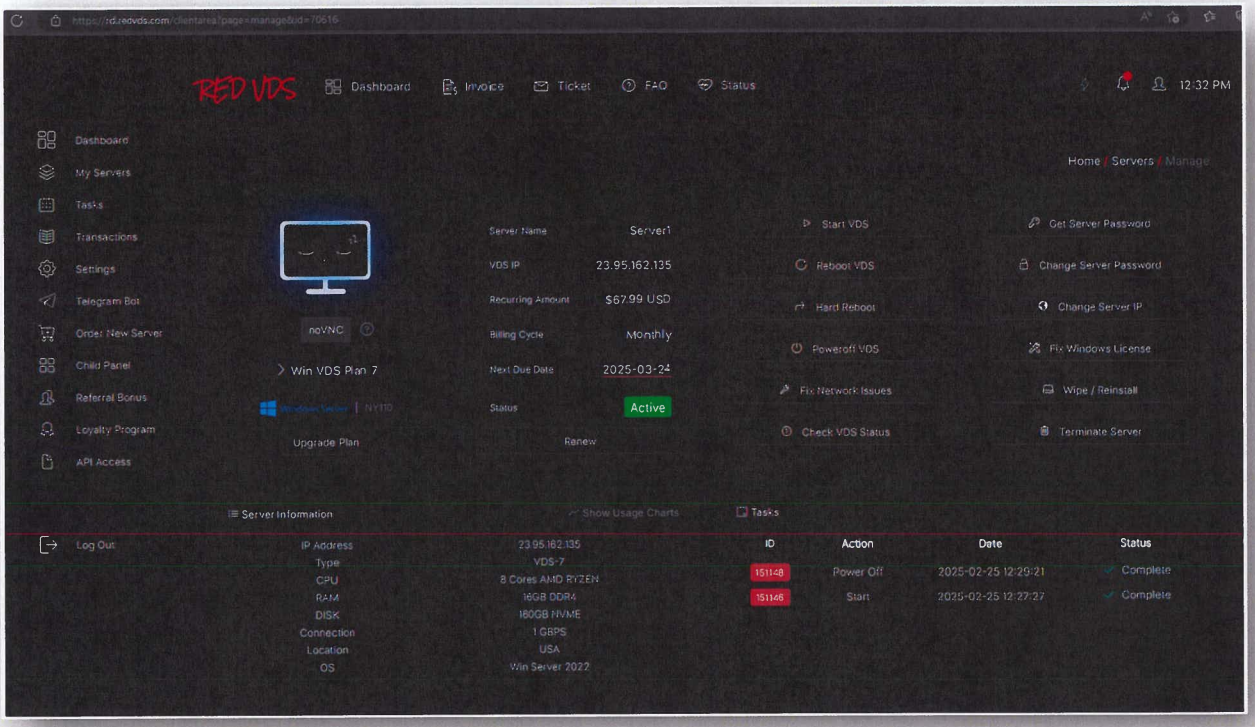
Windows Server software licenses are sold through channels designed to meet the unique needs of customers. Keating Decl. ¶6. These sales channels include online retailers offering full packaged product (FPP) licenses of Windows Server software, original equipment manufacturers (OEMs) offering pre-installed licenses with their hardware systems, as well as Licensing Solutions Partners (LSPs) and Enterprise Software Advisors (ESAs) offering Windows Server software through Microsoft Commercial Licensing programs. *Id.*

The current version of Windows Server is Windows Sever 2025. There are three versions of Windows Server 2025 commercially licensed by Microsoft. *Id.* ¶7. Windows Server Data Center Edition is ideal for highly virtualized and software-defined datacenter environments. Standard edition is ideal for customers with low density or non-virtualized environments. Essentials edition is a cloud-connected first server, ideal for small businesses with up to 25 users and 50 devices. Windows Server 2025 Essentials edition is available to purchase from OEMs only. *Id.*¶ 7. In addition to commercially licensed versions of Windows Server, Microsoft also licenses evaluation versions of Windows Server for customers who wish to evaluate the software before entering into a commercial license. *Id.* ¶ 12. Evaluation versions of Windows Server must be activated over the internet in the first 10 days to avoid automatic shutdown. *Id.*¶ 12.

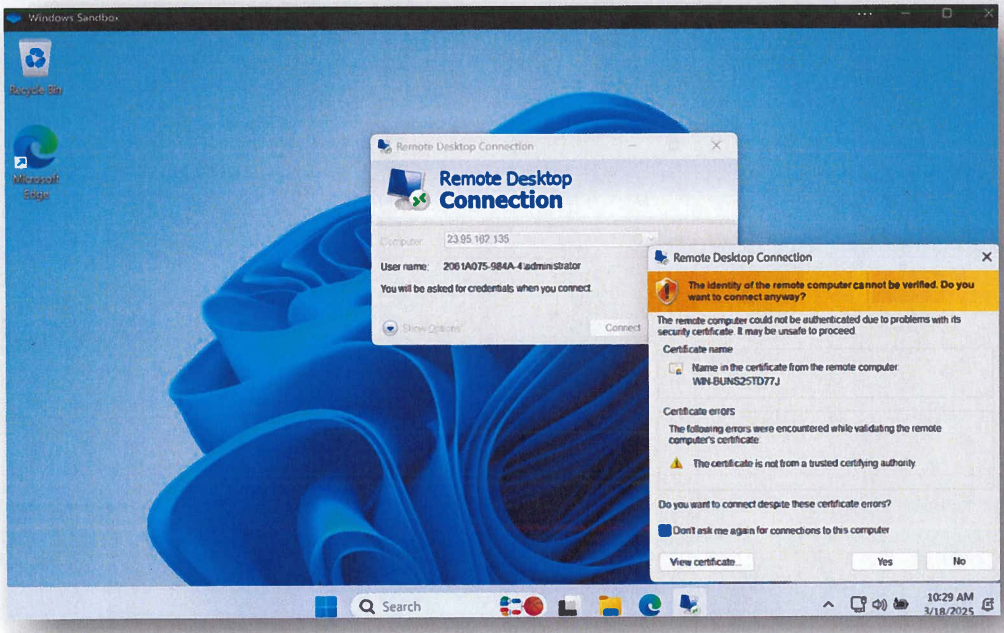
At some point prior to 2023, RedVDS obtained an evaluation copy of Windows Server 2022 from Microsoft or a third party. The copy of Windows Server obtained by RedVDS contains an embedded evaluation Windows Server Key that enables 180 days of usage; after 180 days of usage, a user receives a message informing them that their evaluation license has expired and prompting them to obtain a proper usage license. *Id.* ¶14. RedVDS unlawfully cloned this copy of Windows Server and its embeded Windows Sever Evaluation key in order to enable an unlimited number of users to run copies of the cloned RedVDS Windows Server instance. *Id.*

RedVDS installed one copy of Windows Server onto a virtual computer with the identifying Computer Net Bios Name "WIN-BUNS25TD77J". RedVDS then created numerous images of this virtual computer for distribution across a variety of hosting sites in locations all over the world. RedVDS offers unauthorized copies of Windows Server in a virtual environment that can be remotely accessed from any computer connected to the internet. Keating Decl. ¶ 13. The "VDS" in RedVDS stands for "virtual desktop server" because it allows users to remotely access a virtual Windows desktop that can then be used as a server to facilitate network operations for multiple computers. *Id.*¶ 13. For example, a user can use one computer to remote into a RedVDS virtual Windows Server running on a different computer and use that Windows Server computer as a hub for controlling networks of other computers. *Id.* RedVDS engages the services of other third-party hosting providers and installs unauthorized copies of Windows Server on those hosting providers' servers. RedVDS then sells access to these copies of Windows Server to end users. Declaration of Maurice Mason ("Mason Decl.") ¶ 4-5. RedVDS end users are engaged in illegal activities like phishing, business email compromise fraud schemes, and other cybercrime activities that often involve gaining unauthorized access to computer systems and data. Ensz Dec. ¶ 11.

RedVDS's user interface makes prominent use of Microsoft's Windows trademarks and logo. Ensz Decl. ¶ 25. Figure 2 from the Declaration of Sean Ensz depicts the RedVDS user interface displaying Microsoft's trademarks and Windows logo:



Figures 3 and 4 of Mr. Ensz's declaration show the pirated Windows Server 2022 interface encountered by users of RedVDS upon execution of a RedVDS instance.



Continuity, Structure, and Patterns of the RedVDS Enterprise

Commencing in 2024, Microsoft observed the existence of numerous malicious Windows virtual hosts, all using the same host name of "WIN-BUNS25TD77J". Ensz Decl. ¶ 24. Further investigation revealed that the WIN-BUNS25TD77J identifier is associated with thousands of stolen credentials, invoices, mass mailers, and phish kits. Microsoft determined that the host machines associated with WIN-BUNS25TD77J were all created from the same virtual computer image. These images contain the cloned evaluation copy of Windows Server 2022 discussed above. Microsoft eventually traced these cloned evaluation copies to the RedVDS Domains. Ensz Decl. ¶ 24; Keating Decl. ¶¶ 18-19.

Defendant **DOE 1** controls the RedVDS Domains and source copy of the Windows Server. RedVDS Domains host webpages that include a user portal that can be used to control virtual instances of Windows Server, webpages that facilitate end user purchases of additional unauthorized instances of Windows Server, and webpages offering customer support through

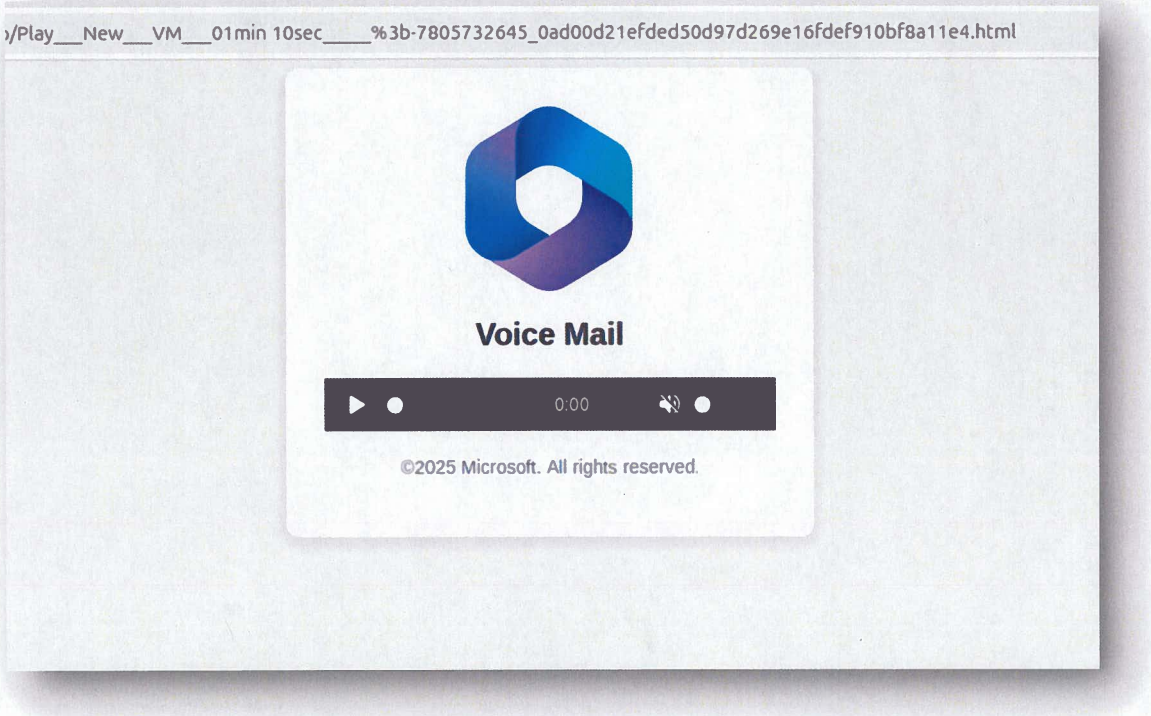
chat sessions and a chat bot. The RedVDS Domains also facilitate API functionality that permits users to control numerous computers at scale. The RedVDS Domains also facilitate a referral bonus program and loyalty program through which end users can share in the ill-gotten profits generated by the RedVDS Enterprise. Enzs Decl. ¶12.

Defendant **DOE 2** is a natural person who makes ongoing use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. DOE 2 operates these types of fraudulent email campaigns at scale, resulting in transmission of thousands of emails containing false and misleading depictions of Microsoft's trademarks. DOE 2 is the individual principally responsible for defrauding GDCA of several hundred thousand dollars. Enzs Decl. ¶ 13. Defendant **DOE 3** is a natural person who makes ongoing use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States. DOE 3 is the individual principally responsible for defrauding H2 of several million dollars. Enzs Decl. ¶ 14. **DOES 4-7** are natural persons who makes ongoing use of the RedVDS Enterprise's services to send fraudulent emails to and from recipients located in the United States at scale, resulting in transmission of thousands of emails containing false and misleading attachments in furtherance of unauthorized email account takeover schemes targeting a wide range of entities including numerous participants in Real Estate, Construction, Insurance, Accounting, Manufacturing, Educational institutions across the United States. Ensz Decl. ¶¶ 15-18.

End users purchasing and using services from the RedVDS Enterprise typically tender payment to DOE 1 via one or more crypto wallets. Declaration of Maurice Mason ("Mason Decl.") ¶¶4-5. DOE 1 has received over $5.3MM of BTC and LTC cryptocurrency payments since June 2023, and it is likely that DOE 1 has made much more money this year in the form of

other cryptocurrency payments. *Id.* ¶¶21-23. After receiving payment, the RedVDS Enterprise deploys an automated process to create a virtual machine for the end user using the image and copy of Windows Server 2022 discussed above. *Id.* ¶8. End users then use the virtual machine image, Windows Server software, and hosting services provided by the RedVDS Enterprise to remotely access and control a virtual computers for malicious purposes. *Id.*

In the course of carrying out their scheme, RedVDS users unlawfully use Microsoft's copyright protected software and/or Microsoft's well-known trademarks to carry out various forms of wire fraud. For example, Figure 6 from the Declaration of Sean Ensz shows DOE 2's misuse of the MICROSOFT® word mark and Microsoft 365 logo:



Investigation into the RedVDS Domains revealed that RedVDS is not a registered company or legal entity in any state or nation. The Terms of Service indicate it is governed by Bahamian Law, and the domain registration for the RedVDS URL provides what appears to be a fake name ("David Rico") and fake address. For example, the domain registrant address given

for RedVDS corresponds to a University of the Bahamas International Building that was slated for demolition in 2024. Ensz Decl.¶ 30; Keating Decl.¶19.

The use of fake name and address information is consistent with trade craft commonly used by perpetrators of ongoing software piracy and cybercrime schemes. Ensz Decl. ¶ 30. Other elements of RedVDS trade craft consistent with ongoing cybercriminal practices include the use of attachments and file types associated with known copyrighted software and well-known company trademarks. *Id.* ¶32. In addition, reports indicate the use of AI tools by persons associated with the RedVDS infrastructures. One victim report indicates the use of AI voice generation tools to impersonate individuals and further deceive recipients of such email communications. Artificial intelligence tactics like face-swapping and voice cloning services are increasingly used by criminals, in particular actors engaged in fraud and scams, to impersonate others and to conceal their true identities, all for the purpose of deceiving victims. *Id.* ¶ 33.

The conduct of the RedVDS Enterprise is ongoing. DOE 1 continues to sell pirated versions of Windows Server 2022. DOE 1 also continues to assist RedVDS end users in circumventing Microsoft's licensing system to run pirated copies of Window Server, and DOES 2-7 continue to have access to the tools used to operate BEC attacks and other malicious activities via the RedVDS service at scale. Defendants are carrying out their scheme throughout the United States, including in the state of Florida. Ensz Decl. ¶ 19.

ARGUMENT

I. THE COURT HAS JURISDICTION OVER DEFENDANTS AND THEIR INSTRUMENTALITIES

The Court has federal question subject matter jurisdiction over Plaintiffs federal claims and also has supplemental jurisdiction over Florida state-law claims pursuant to 28 U.S.C. § 1367. The Court has personal jurisdiction over Defendants because in carrying out the conduct described in this Complaint, Defendants have availed themselves of the privilege of conducting

business in Florida. *See, e.g., Diamond Crystal Brands, Inc. v. Food Movers Int'l*, 593 F.3d 1249, 1267 (11th Cir. 2010).

First, Defendants have intentionally extracted data from Florida corporations and used that data to send fraudulent communications to the corporations' employees. Second, Defendants have intentionally used servers located in Florida and services provided ReliableSite.Net LLC, a U.S. company headquartered in Miami, Florida, in order to run the unauthorized copies of Windows Server at issue, and to use those instances of Windows Server to carry out BECs and financial fraud. Defendants have thus acted within the state and directed the acts complained toward the State, its residents, and this judicial district. *See, e.g., Skyhop Techs., Inc. v. Narra*, 58 F.4th 1211, 1228 (11th Cir. 2023) ("SkyHop's CFAA claim arises from Indyzen's communications into Florida"); *United States v. Auernheimer*, 748 F.3d 525, 533 (3d Cir. 2014) (Venue would be proper in any district where the CFAA violation occurred, or wherever any of the acts in furtherance of the conspiracy took place.").

In addition to their contacts with Florida, Defendants also have sufficient national contacts with the United States as a whole to subject each Defendant to the Court's jurisdiction consistent with requirements of due process. *See, e.g., Charter Oil Co. v. Cotton (In re Charter Oil Co.)*, 189 B.R. 527, 530 (Bankr. M.D. Fla. 1995) ("The national contacts analysis requires that defendants have national contacts with the United States, not the State'). Defendants have acted at all times relevant with knowledge that their acts would cause harm through computers located in Florida, thereby injuring Plaintiffs and others in in the United States. Further, Defendants intentionally availed themselves of the privilege of doing business in the United States by engaging in the following activities:

- fraudulently gaining access to Microsoft's Windows Server software, which required one or more Defendants to affirmatively enter into license agreements with Microsoft by misrepresenting that they would not use Microsoft's materials for illegal purposes;

- Contracting with and utilizing the services of Cloudflare, Inc., a U.S. company headquartered in San Francisco, California that provides network infrastructure and proxy services,
- Contracting with and utilizing the services of Interserver, Inc., a U.S. hosting company headquartered in New Jersey
- Contracting with and utilizing the services of ReliableSite.Net LLC, a U.S. company headquartered in Miami, Florida.
- Contracting with and utilizing the services of Verisign, Inc., a U.S. domain registry.
- Contracting with and utilizing the services of Identity Digital, Inc., a U.S. domain registry.
- Using the U.S. wires to transmit computer commands and electronic communications to victim computers;
- Targeting and victimizing U.S. companies, organizations, and persons, as discussed below.

Ensz Decl. ¶ 20. Accordingly, to the extent Defendants do not have sufficient contacts with Florida alone to support jurisdiction and venue in this Court, each Defendant is subject to jurisdiction based on their national contacts with the United States and are thus subject to national service of process and jurisdiction is proper in this Court. *Gen. Cigar Holdings, Inc. v. Altadis, S.A.*, 205 F. Supp. 2d 1335, 1340 (S.D. Fla. 2002) ("personal jurisdiction is proper in any district, so long as sufficient national contacts have been established."); *Republic of Pan. v. BCCI Holdings (Luxembourg) S.A.*, 119 F.3d 935, 942 (11th Cir. 1997) ("Section 1965(d) of the RICO statute provides for service in any judicial district in which the defendant is found.").

II. THE RECORD SUPPORTS A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTIVE RELIEF

The fundamental purpose of a preliminary injunction is to prevent irreparable harm during the pendency of a lawsuit and to preserve the court's ability to render a meaningful judgment on the merits. *See, e.g., United States v. State of Ala.*, 791 F.2d 1450, 1459 (11th Cir.

1986). "Parties seeking a preliminary injunction must demonstrate that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm, (3) the balance of hardships tips in their favor, and (4) the injunction is in the public interest. *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)). Here, Defendants' conduct causes irreparable harm to Microsoft because Defendants are facilitating malicious misuse of Microsoft's trademarks and copyrighted materials, and using Microsoft's IP deceive innocent victims. Defendants are also using their malicious infrastructure and services to gain unauthorized access to computer and email systems, causing harm to victims like H2 and GDCA. Each of these is a distinct and cognizable form of irreparable harm. *See, e.g., Fla. Atl. Univ. Bd. of Trs. v. Parsont*, 465 F. Supp. 3d 1279 (S.D. Fla. 2020) (granting preliminary injunction because "federal courts around the country agree that the interference with an entity's control of its computer systems constitutes irreparable injury"); *Metro-Goldwyn-Mayer, Inc. v. Showcase Atlanta Co-op. Prods., Inc.*, 479 F. Supp. 351 (N.D. Ga. 1979) (copyright infringement as irreparable harm); *Boulan S. Beach Master Ass'n, Inc. v. Think Pro*ps., LLC, 617 F. App'x 931 (11th Cir. 2015) (vacating district court's denial of a preliminary injunction when plaintiff pled that trademark misuse caused confusion and damage to its brand). Every day that passes gives Defendants an opportunity to cause more damage. Unless the requested relief is granted, Defendants will continue to use the RedVDS infrastructure to infringe Microsoft's intellectual property and gain unauthorized access to the contents of private communications transmitted through protected computer systems, all in furtherance of financial fraud like that suffered by H2 and GDCA.

A. Plaintiffs Are Likely to Succeed on the Merits of their Claims

Plaintiffs' evidence shows they will be able to establish the elements of each of their claims. Given the strength of Plaintiffs' evidence, the likelihood of success on the merits weighs heavily in favor of granting injunctive relief.

CFAA. Congress enacted the CFAA specifically to address computer crime. *See, e.g., Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010); *Big Rock Sports, LLC v. AcuSport Corp.*, 2011 U.S. Dist. LEXIS 110995, *3 (E.D.N.C. Sept. 26,

2011). "Any computer with Internet access [is] subject [to] the statute's protection." *Id.*; *United States v. Gasperini*, 2017 WL 2399693, at *3 (E.D.N.Y. June 1, 2017); *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 608 (E.D. Va. 2005). *Inter alia,* the CFAA penalizes a party that intentionally accesses a protected computer without authorization in furtherance of a scheme to defraud. 18 U.S.C. § 1030(a)(4). That is exactly what Defendants did when they accessed the computers that run the email systems of H2, GDCA, and their respective counterparties are protected computers. Noyes Decl. ¶¶ 4, 9; Blackwell Decl. ¶¶ 5, 9; Ensz Decl. ¶¶ 12-14. Defendants systematic use of social engineering to trick users and gain unauthorized access to victims' computers and data in furtherance of financial fraud schemes represent quintessential CFAA violations. *See, e.g., Microsoft Corp. v. Does 1-51*, No. 1:17-CV-4566, 2017 WL 10087886 at *4 (N.D. Ga. Nov. 17, 2017);*Volk v. Zeanah,* No. 608CV094, 2010 U.S. Dist. LEXIS 5621, at *4 (S.D. Ga. Jan. 25, 2010) ("The CFAA is meant to reduce hacking of computer systems/networks"); *Schwartz v. ADP, Inc.*, No. 2:21-cv-283-SPC-MRM, 2021 U.S. Dist. LEXIS 231613, at *3 (M.D. Fla. Dec. 3, 2021) ("The CFAA punishes computer hacking"). Defendants' conduct has caused harm to H2 and GDCA far exceeding the $5,000 jurisdictional threshold. Noyes Decl. ¶ 16; Blackwell Decl. ¶13.

ECPA Claims. Like the CFAA, the ECPA is "primarily a criminal statute with a civil component aimed at creating a private right of action against computer hackers and electronic trespassers. *St. Johns Vein Ctr. v. StreamlineMD Ltd. Liab. Co.*, 347 F. Supp. 3d 1047, 1063 n.16 (M.D. Fla. 2018) (quoting *IPC Sys. v. Garrigan*, No. 1:11-CV-3910-AT, 2012 U.S. Dist. LEXIS 195619, at *24-25 (N.D. Ga. May 21, 2012)). The ECPA "makes it unlawful for anyone to "(1) intentionally access[] without authorization a facility through which an electronic communication services is provided; or (2) intentionally exceed[] an authorization to access that facility; and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a). Section 2701 may be enforced in a civil action brought by "any…person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or

intentional state of mind." 18 U.S.C. § 2707(a). Defendants conduct "violates the ECPA because Defendants break into computing devices and computer networks with the direct intention of acquiring the contents of sensitive communications such as e-mails, voice mails, or other communications types." *Microsoft Corp. v. Does*, Civil Action No. 1:16cv993, 2017 U.S. Dist. LEXIS 145448, at *13 (E.D. Va. Aug. 1, 2017); Ensz Decl. ¶¶ 12-14. H2 and GDCA both suffered losses because of Defendants ECPA violations and unlawful access to their private communications with business partners. Noyes Decl. ¶¶ 4, 9; Blackwell Decl. ¶¶ 5, 9; Ensz Decl. ¶¶ 12-14.

Lanham Act Claims. Defendants' conduct constitutes numerous violations of the Lanham Act, including false designation of origin under section 1125(a), which prohibits use of a registered mark that is likely to deceive as to the affiliation, connection, or association of such person with another person. 15 U.S.C. § 1125(a)(1)(A). Here, Defendants' social engineering campaigns leverage Microsoft's trademarks and logos to make it look like the messages are legitimate communications from Microsoft. Ensz Decl. ¶¶ 25-26 & 29. Such misuse of Microsoft's trademarks is a clear violation of Lanham Act § 1125(a) and Microsoft is likely to succeed on the merits. *See Garden & Gun, LLC v. Twodalgals, LLC*, 2008 U.S. Dist. LEXIS 79982 (W.D.N.C. 2008). Where, as here, a defendant uses a plainitff's trademark "likely to cause confusion, or to cause mistake, or to deceive," infringement is established. *E.g., Aeropost Int'l Servs. v. Aerocasillas, S.A.*, No. 09-23437-CIV-MORE, 2011 U.S. Dist. LEXIS 165635, at *26 (S.D. Fla. Mar. 31, 2011).

In addition, Defendants distribute pirated, gray market versions of Windows Server and used Microsoft's trademarks to advertise and operate the RedVDS service. Ensz Decl. ¶__, *see, e.g., Microsoft Corp. v. Tierra Comput., Inc.*, 184 F. Supp. 2d 1329, 1333 (N.D. Ga. 2001) ("Defendants used counterfeit marks in the sale of the infringing software packages"). In doing so, Defendants display Microsoft's trademarks in a manner that infringes and warrants injunctive relief. *E.g., Sueros & Bebidas Rehidratantes, S.A. de C.V. v. El Boqueron Imps. LLC,* No. 1:24-cv-03874-TWT, 2025 U.S. Dist. LEXIS 201965, at *8 (N.D. Ga. Oct. 10, 2025).

Copyright Act Claims. Under § 106(3) of the Copyright Act, a copyright owner "has the exclusive rights…to distribute copies … of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending." 17 U.S.C. §106(3). *Microsoft Corp. v. Big Boy Distribution Ltd. Liab. Co.*, 589 F. Supp. 2d 1308, 1315 (S.D. Fla. 2008). A certificate of registration from the U.S. Copyright Office is prima facie evidence of a copyright's validity. *See Glennon v. Rosenblum*, 325 F. Supp. 3d 1255, 1263 (N.D. Ala. 2018). Here, Microsoft holds a registration for Windows Server 2022, which Defendants are reproducing and distributing without authorization. Keating Decl. ¶¶ 13-17. The elements of copyright infringement have thus been established. *See, e.g., Microsoft Corp. v. Big Boy Distribution Ltd. Liab. Co.*, 589 F. Supp. 2d 1308, 1318, 21 (S.D. Fla. 2008); *Microsoft Corp. v. Silver Star Micro, Inc.,* No. 1:06-cv-1350-WSD, 2008 U.S. Dist. LEXIS 1526, at *18 (N.D. Ga. Jan. 9, 2008) ("evidence here establishes that the Defendants duplicated Microsoft [software] without authorization and therefore infringed on Plaintiff's copyrights on that software.").

RICO Claims. To succeed on a civil RICO claim, a private RICO plaintiff must allege "(1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity." *Viridis Corp. v. TCA Glob. Credit Master Fund, LP*, 155 F. Supp. 3d 1344, 1354 (S.D. Fla. 2015) (citation omitted). "Racketeering activity" includes any act violative of several specific federal statutes, including 18 U.S.C. § 1343 wire fraud, 18 U.S.C. § 2319 criminal copyright infringement, and 18 U.S.C. § 2320 criminal trademark infringement. 18 U.S.C § 1961. A civil RICO plaintiff must also show that multiple acts of racketeering "(5) caused (6) injury to the business or property of the plaintiff." *Cisneros v. Petland, Inc.*, 972 F.3d 1204, 1211 (11th Cir. 2020).

Plaintiffs' evidence shows that Defendants are members of an ongoing association-in-fact enterprise who participants in the conduct of a the RedVDS Enterprise. Ensz Decl. ¶¶ 10-29. Defendants have conducted the affairs of the Enterprise through a coordinated and continuous pattern of illegal activity in order to achieve their common unlawful purposes. For example, Defendants exchange referral fees and services in furtherance of the pattern of copyright and trademark infringement for financial gain carried out via the RedVDS Domains. Ensz Decl.¶ 12.

Defendants have also engaged in racketeering by violating the federal wire fraud by repeatedly using the Internet to engage in financial fraud against entities like GDCA and H2. *See, e.g., United States v. Azari*, No. 19-cr-610 (JGK), 2024 U.S. Dist. LEXIS 165416, at *1 (S.D.N.Y. Sep. 10, 2024); *United States v. 113 Virtual Currency Accounts*, Civil Action No. 20-606, 2020 U.S. Dist. LEXIS 142015, at *2 (D.D.C. Aug. 4, 2020) ("the hacking and theft of virtual currencies in violation of 18 U.S.C. § 1343").

Conversion. Under Florida law, "withdrawing money from an account and exercising wrongful dominion and control over the money is an act of conversion." *Engineered Yacht Sols., Inc. v. Cohoon,* No. 24-61869-CIV/SINGHAL, 2025 U.S. Dist. LEXIS 124951, at *7 (S.D. Fla. June 30, 2025)(citations omitted). H2 and GDCA have each established clear, meritorious claims for conversion against Defendants involving substantial amounts of money.

B. Defendants' Conduct Causes Irreparable Harm

Defendants' conduct causes several types of irreparable harm. First, "[n]umerous courts have found that unauthorized access of computers and the acquisition of data in violation of the CFAA constitute irreparable harm." *Chegg, Inc. v. Doe,* No. 22-cv-07326-CRB, 2023 U.S. Dist. LEXIS 200023, at *21-22 (N.D. Cal. Nov. 7, 2023) (collecting cases); *Microsoft Corp. v. Does 1-51*, No. 1:17-CV-4566, 2017 WL 10087886 at *2 (N.D. Ga. Nov. 17, 2017); *see also, e.g., Microsoft Corp. v. Does*, Civil Action No. 1:21-cv-822 RDA/IDD, 2022 U.S. Dist. LEXIS 236135, at *11-12 (E.D. Va. Dec. 27, 2022) (citing *Microsoft Corp. v. Peng Yong et al.*, Case No. 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (injunction to dismantle botnet command and control servers); and *Microsoft v. Piatti, et al.*, Case No. 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (injunction [*12] to dismantle botnet command and control servers)); accord *Microsoft Corp. v. John Does 1-27*, Case No. 1:10-cv-156 (E.D. Va. 2010, Brinkema J.) (similar).

Second, it is well settled that consumer confusion and injury to business goodwill constitute irreparable harm. *See, e.g., Badia Spices, Inc. v. Gel Spice Co.,* No. 15-CV-24391-COOKE/LOUIS, 2019 U.S. Dist. LEXIS 113626, at *12 (S.D. Fla. July 8, 2019); *Int'l Labor*

Mgmt. Corp. v. Perez, 2014 U.S. Dist. LEXIS 57803, 35 (M.D.N.C. Apr. 25, 2014) (damage to "reputation and loss of goodwill constitutes irreparable harm for purposes of injunctive relief") (citing *In Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546 (4th Cir. 1994)); *MicroAire Surgical Instruments, LLC v. Arthrex, Inc.*, 726 F. Supp. 2d 604, 635 (W.D. Va. 2010) ("The loss of goodwill is a well-recognized basis for finding irreparable harm"). A finding of irreparable harm usually follows a finding of unlawful use of a trademark and a likelihood of confusion. *Ledo Pizza Sys. v. Singh*, 2013 U.S. Dist. LEXIS 146938, 9 (D. Md. Oct. 10, 2013); *Nabisco Brands, Inc. v. Conusa Corp.*, 722 F. Supp. 1287, 1290 (M.D.N.C. 1989) ("In the context of a trademark infringement dispute, several courts have held that where likelihood of confusion is established likelihood of success on the merits as well as risk of irreparable harm follow.").

Here, Defendants' conduct tarnishes Microsoft's valuable trademarks, injuring Microsoft's goodwill, creating confusion as to the source of harmful content created or facilitated by Defendants, and damaging the reputation of Microsoft and the public's confidence in Microsoft's robust safety measures. Defendants are also depriving Microsoft of the right to control the use, distribution, and modification of its copyrighted software code. *See, e.g., Compulife Software Inc. v. Newman*, 959 F.3d 1288 (11th Cir. 2020). These injuries are sufficient in and of themselves to constitute irreparable harm.

Lastly, as a practical matter, Defendants are causing harm that is unlikely to ever be compensated by monetary payment—even after final judgment—because Defendants are elusive cybercriminals whom Plaintiffs are unlikely to be able to enforce judgments against. "[C]ircumstances[] such as insolvency or unsatisfiability of a money judgment, can show irreparable harm." *Khepera-Bey v. Santander Consumer USA, Inc.*, 2013 U.S. Dist. LEXIS 87641, 13-14 (D. Md. June 21, 2013); accord *Burns v. Dennis-Lambert Invs., Ltd. P'ship*, 2012 Bankr. LEXIS 1107, 9 (Bankr. M.D.N.C. Mar. 15, 2012) ("a preliminary injunction may be appropriate where 'damages may be unobtainable from the defendant because he may become insolvent before final judgment can be entered.'"); *Rudolph v. Beacon Indep. Living LLC*, 2012

U.S. Dist. LEXIS 7075, 5 (W.D.N.C. Jan. 23, 2012) ("Irreparable harm exists here because of Defendant Beacon's continued occupancy of the Facility without paying any rents, particularly in light of the threat of insolvency by one or more Defendants.").

C. The Balance of Equities Strongly Favors Injunctive Relief

Because Defendants are engaged in an illegal scheme to obtain unlawful access to computer and communications systems, commit financial fraud, and create and disseminate infringing materials, the balance of equities clearly tips in favor granting an injunction. *See, e.g., Badia Spices,* 2019 U.S. Dist. LEXIS 113626, at *12; *US Airways, Inc. v. US Airline Pilots Ass'n*, 813 F. Supp. 2d 710, 736 (W.D.N.C. 2011); *Pesch v. First City Bank of Dallas*, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (balance of hardships clearly favors injunction where enjoined activity is illegal). On one side of the scales of equity rests the harm to Plaintiffs and the public at large, while on the other side rests no legally cognizable harm to Defendants because an injunction would only require them to cease illegal activities. *US Airways*, 13 F. Supp. 2d at 736.

D. The Public Interest Favors an Injunction

The public has a strong interest in enforcing laws like the CFAA, ECPA, RICO ACT, Copyright Act, and Lanham Act. *See, e.g., Sream, Inc. v. Barakat Food, Inc.*, No. 16-24722-CV, 2017 U.S. Dist. LEXIS 165420, at *8 (S.D. Fla. Oct. 4, 2017) (public interest in intellectual property protection); *ProFitness Phys. Therapy Ctr. v. Pro-Fit Ortho. And Sports Phys. Therapy P.C.*, 314 F.3d 62, 68 (2d Cir. 2002) (same); *BSN Med., Inc. v. Art Witkowski*, 2008 U.S. Dist. LEXIS 95338, 10 (W.D.N.C. Nov. 21, 2008) ("In a trademark case, the public interest is 'most often a synonym for the right of the public not to be deceived or confused.' . . . the infringer's use damages the public interest.") (citation omitted); *accord Meineke Car Care Ctrs., Inc. v. Bica*, 2011 U.S. Dist. LEXIS 118171, 10 (W.D.N.C. Oct. 12, 2011) (similar); *Google LLC v. Starovikov,* Civil Action No. 1:21-cv-10260-DLC, 2021 U.S. Dist. LEXIS 252274, at *10 (S.D.N.Y. Dec. 16, 2021) ("public interest is clearly served by enforcing statutes designed to protect the public, such as RICO, the CFAA, the ECPA, and the Lanham Act"); *FXDirectDealer,*

LLC v. Abadi, 2012 WL 1155139, at *8 (S.D.N.Y. Apr. 5, 2012) (public interest weighed in favor of injunction to enforce CFAA); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 32 (E.D. Va. Jan. 6, 2014) (same); . The public also has a strong interest in disrupting criminal enterprises operating in violation of the RICO Act. *See, e.g., Amazon.com, Inc. v. WDC Holdings LLC*, Civil Action No. 1:20-cv-484, 2020 U.S. Dist. LEXIS 134555, at *31 (E.D. Va. July 28, 2020) (granting injunction to enjoin RICO enterprise conduct). "Microsoft's proposed injunction is tailored to target and disable communication between Defendants" and to disrupt the malicious infrastructure at issue "with the least amount of burden on third party domain registries and the public," which ensures that "the public interest would not be harmed, and likely would be served, by a permanent injunction." *Microsoft Corp. v. Doe*, No. 20-CV-1217 (LDH) (RER), 2021 U.S. Dist. LEXIS 101862, at *28 (E.D.N.Y. May 28, 2021).

E. The All Writs Act Authorizes the Court to Direct Third Parties to Perform Acts Necessary to Avoid Frustration of the Requested Relief

Microsoft's Proposed Order directs that the third-party service providers whose infrastructure Defendants rely on to reasonably cooperate to effectuate the order. Microsoft's proposed order also directs such entities to preserve evidence of Defendants' conduct. Microsoft has been working with private and public partners regarding remediation of Defendants misconduct, and several third-party entities are inclined to assist in removing illegal and abusive accounts from their respective services. Microsoft has observed voluntary third-party compliance with orders like the one it seeks here in several past cases, which makes sense because it is in most companies' interests to reduce the amount of cybercrime carried out on their platforms.

In addition to the fact that many third parties are likely to voluntarily comply with orders such as the one Microsoft seeks here, the All Writs Act provides a mechanism for obtaining compliance if needed. The Act provides that a court may issue all writs necessary or appropriate for the administration of justice. 28 U.S.C. § 1651(a). The Supreme Court has recognized that

narrow direction to third parties necessary to effect the implementation of a court order is authorized by the All Writs Act:

The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, and encompasses even those who have not taken any affirmative action to hinder justice.

United States v. New York Tel. Co., 434 U.S. at 174 (citations omitted) (order to telephone company to assist in implementation of a pen register warrant was authorized under the All Writs Act); *Microsoft Corp. v. Doe*, 2014 U.S. Dist. LEXIS 48398, 30 (E.D. Va. Jan. 6, 2014) (invoking All Writs act and granting relief similar to that requested herein); *United States v. X,* 601 F. Supp. 1039, 1042 (D. Md. 1984) (All Writs Act permits the district court to order a third party to provide "nonburdensome technical assistance" in aid of valid warrant); *Moore v. Tangipahoa Parish Sch. Bd.,* 507 Fed. App'x. 389, 396 (5th Cir. 2013) (unpublished) ("The All Writs Act provides 'power to a federal court to issue such commands . . . as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained.'") (citing *New York Tel. Co.,* 434 U.S. at 172); *see also In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities*, 616 F.2d 1122, 1129 (9th Cir. 1980) (same; noting of New York Tel. Co., "the Court made the commonsense observation that, without the participation of the telephone company, 'there is no conceivable way in which the surveillance authorized could have been successfully accomplished.'" 434 U.S. at 172); *In re Baldwin-United Corp.*, 770 F.2d 328, 338-339 (2d Cir. 1985) ("An important feature of the All-Writs Act is its grant of authority to enjoin and bind non-parties to an action when needed to preserve the court's ability to reach or enforce its decision in a case over which it has proper jurisdiction"; "We do not believe that Rule 65 was intended to impose such a limit on the court's authority provided by the All-Writs Act to protect its ability to render a binding judgment."); *Dell Inc.*, 2007 U.S. Dist. LEXIS 98676, at *16 (All Writs Act applied in conjunction with trademark seizure under Rule 65).

Requiring the third parties whose domains are within the Court's power under the all writs act because compliance (1) requires only minimal assistance from such third parties in executing the order (acts that they would take in the ordinary course of their operations upon receipt of abuse notifications), (2) requires that it be implemented with the least degree of interference with the normal operation of third parties, (3) does not deprive of any tangible or significant property interests and (4) requires Microsoft to compensate for costs, if any, associated with the assistance rendered. If, in the implementation of the Proposed Order, any third party wishes to bring an issue to the attention of the Court, Microsoft will bring it immediately. All affected parties will have an opportunity to be heard at the preliminary injunction hearing, which must occur shortly after the execution of the Proposed Order. Fed. R. Civ. P. 65(b)(2). The third-party directions in the Proposed Order are thus narrow, satisfy Due Process, and are necessary to ensure that the relief is not rendered fruitless.

F. An Ex Parte TRO that Remains Sealed for a Limited Time Is the Only Effective Means of Relief

The Orders Microsoft requests herein must issue ex parte for the relief to be effective at all because of the extraordinary factual circumstances here—namely, Defendants' technical sophistication and ability to move their infrastructure and evidence if given advance notice of Microsoft's request for injunctive relief. Rule 65 of the Federal Rules of Civil Procedure permits an ex parte TRO where the moving party sets forth facts that show an immediate and irreparable injury and why notice should not be required. Fed. R. Civ. P. 65(b)(1); see *Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers*, Lcal No. 70, 415 U.S. 423, 438-39 (1974) ("Ex parte temporary restraining orders are no doubt necessary in certain circumstances[.]"). If notice is given prior to issuance of a TRO, it is likely that Defendants will be able to relocate or conceal their infrastructure and associated artifacts before Microsoft can obtain discovery and before the TRO can have any remedial effects. Ensz Decl. ¶ 37. Ex parte

relief is appropriate under circumstances such as the instant case, where notice would render the requested relief ineffective. *See, e.g., Microsoft Corp. v. Does 1-51*, No. 1:17-CV-4566, 2017 WL 10087886 at *2 (N.D. Ga. Nov. 17, 2017) (granting an ex parte TRO where there was "good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants"); *AllscriptsMisys, LLC v. Am. Digital Networks*, LLC, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (granting an ex parte TRO where "Defendant may dissipate the funds and/or take action to render it difficult to recover funds ...."); *Crosby v. Petromed, Inc.*, 2:09-cv-05055, 2009 U.S. Dist. LEXIS 73419, at *5 (E.D. Wash. Aug. 6, 2009) (granting ex parte TRO as "notice to Defendants of this TRO request could result in further injury or damage to Plaintiffs...."); *AT&T Broadband v. Tech Commc'ns, Inc.* 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (affirming ex parte search and seizure order to seize contraband technical equipment, given evidence that in the past defendants and persons similarly situated had secreted evidence once notice given); *In re Vuitton Et Fils S.A.,* 606 F.2d 1, 4-5 (2d Cir. 1979) (per curiam) (holding that notice prior to issuing TRO was not necessary where notice would "serve only to render fruitless further prosecution of the action"; prior experience taught that once one member of the counterfeiting enterprise received notice, contraband would be transferred to another unknown counterfeiter, perpetuating the harm and rendering judicial efforts pointless). Courts have previously found that where, as in the instant case, Defendants' scheme is "in electronic form and subject to quick, easy, untraceable destruction by Defendants," ex parte relief is particularly warranted. *Dell, Inc. v. Belgiumdomains, LLC*, 1:07-cv-22674, 2007 U.S. Dist. Lexis 98676, at *5-6 (S.D. Fla. Nov. 21, 2007).

III. CONCLUSION

For the reasons set forth herein, Plaintiffs respectfully request that this Court grant the requested injunctive relief and order this action to remained sealed for a limited period of time necessary to effect the Court's orders.

LOCAL RULE 7.1 EMERGENCY CERTIFICATION

After reviewing the facts and researching applicable legal principles, I certify that this motion in fact presents a true emergency (as opposed to a matter that may need only expedited treatment) and requires an immediate ruling because the Court would not be able to provide meaningful relief to a critical, non-routine issue after the expiration of seven days. I understand that an unwarranted certification may lead to sanctions.

Dated: January 7, 2026

Respectfully submitted,

Diana Marie Fassbender

Diana Marie Fassbender (Florida Bar No. 17095)
ORRICK, HERRINGTON & SUTCLIFFE LLP
215 NW 24th St, Suite 200
Miami, FL 33127
Tel: (202) 339-8533
dszego@orrick.com

Robert L. Uriarte (*pro hac vice* forthcoming)
ORRICK, HERRINGTON & SUTCLIFFE LLP
355 S. Grand Ave.
Ste. 2700
Los Angeles, CA 90017
Tel: (213) 629-2020
Fax: (213) 612-2499
ruriarte@orrick.com

Ana M. Mendez-Villamil (*pro hac vice* forthcoming)
ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105
Tel: (415) 773-5700
amendez-villamil@orrick.com

Of Counsel:
Richard Boscovich
MICROSOFT CORPORATION
Microsoft Redwest Building C
5600 148th Ave NE
Redmond, Washington 98052
Tel: (425) 704-0867
rbosco@microsoft.com

Attorneys for Plaintiffs